INTRODUCTION TO THE WEIL CONJECTURES

RUNAR ILE

Abstract. Notes to a lecture given at the University of Oslo, January 29, 2004, slightly modified and expanded to accomodate comments and questions which arised during the talk.

1. The conjectures

1.1. **Arithmetic.** Solve

$$y^2 = x^3 - x - 1$$

in integers.
Answer: There are no integer solutions since there are no solutions modulo 3.

Equations with integer coefficients

$$f_1, f_2, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_n]$$

give equations over finite fields by reduction of the coefficients:

$$\overline{f}_1, \overline{f}_2, \dots, \overline{f}_s \in \mathbb{Z}/p\mathbb{Z}[x_1, \dots, x_n]\,.$$

It is easier to solve the latter, and maybe information about solutions in finite fields can help finding integer solutions (this is at present merely a hope, no general Hasse principle is known, etc.).

1.2. **Geometry (what is a variety?)** Let $\overline{k}$ be an algebraically closed field.

$$X = \operatorname{Spec} A$$

is an *affine variety* over $\overline{k}$ if the quotient ring

$$A = \overline{k}[x_1, \dots, x_n]/(f_1, \dots, f_s)\,,$$

which give the global functions on X, is an integral domain. Geometrically this means that X only has one *component*. E.g. for $A = \overline{k}[x, y, z]/(yz, zx, xy)$, X is the union of the three coordinate axes in 3-space, so has three components (and one connected component), and is not an affine variety, and A is not an integral domain.

Date: February 2, 2004.

Acknowledgement. The author is grateful for partial financial support from RCN's Strategic University Program in Pure Mathematics at the Dept. of Mathematics, University of Oslo (No 154077/420).

A point $P = (p_1, \dots, p_n) \in \overline{k}^n$ is contained in $X \Leftrightarrow f_i(P) = 0$ for all i, and

$$\text{closed points } P \in X \leftrightarrow \text{maximal ideals in } A$$

by Hilberts Nullstellensatz.

Non-maximal prime ideals in A are non-closed points in X. Even though one has to regard non-closed points in the constructruction of an étale cohomology theory, in this note non-closed points will only be mentioned in Theorem 1.

A closed set $Z \subseteq X$ in the *Zariski topology* on X is the set of prime ideals containg an ideal $I = (g_1, \dots, g_t) \subseteq A$, in particular this gives the set of closed points in X defined by the equations $g_i = 0$. A basis for the topology on X is given by open affine sub-varieties $X_h = \operatorname{Spec} A[1/h] \hookrightarrow \operatorname{Spec} A$ for non-zero $h \in A$.

A (locally) ringed space $X = (X, \mathcal{O}_X)$ (a topological space X with a sheaf of rings $\mathcal{O}_X$) is a *variety* over $\overline{k}$ if X has a finite open covering of affine varieties over $\overline{k}$, and X is *separated* ("Hausdorff"; the diagonal embedding is closed).

X is a *complete* variety if in addition X is *proper* over $\overline{k}$ ("compact"; $X \to \operatorname{Spec} \overline{k}$ is universally closed).

Example 1. *Homogeneous* $f_1, \dots, f_s$ define a *projective* variety (contained in $\mathbb{P}^{n-1}_{\overline{k}}$). Projective varieties are complete varieties.

There is also a notion of *non-singularity* (e.g. by the Jacobian). A *map* $X \to Y$ of varieties is locally defined by rational functions.

1.3. **The Zeta function.** Assume k is a finite field, $\#k = q$, where q is a power of a prime number p. Fix an algebraic closure $\overline{k}$. Let $X/\overline{k}$ be variety defined by equations with coefficients in k. Put

$$N_1 = \#X(k)$$

where $X(k)$ is the set of (closed) points in X with coordinates in k. Remark that N_1 is a finite number since $\#\mathbb{A}^n_{\overline{k}}(k) = q^n$. Let k_m be the unique extension field of k of degree m, so $\#k_m = q^m$. Set

$$N_m = \#X(k_m)\,.$$

There is also an invariant description of the k_m-points on X. Let X_0 be the scheme defined by the same equations over the field k, so that $X = X_0 \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$, then $X(k_m)$ equals the set of maps $\operatorname{Spec} k_m \to \operatorname{Spec} X_0$ over $\operatorname{Spec} k$.

Definition 1. The *zeta function* of X defined over k is

$$Z(X, t) := \exp \sum_{m \geqslant 1} N_m \frac{t^m}{m} \qquad \in 1 + t \cdot \mathbb{Q}[[t]]\,.$$

1.4. **A. Weil's conjectures.** Assume that $X/\overline{k}$ is a non-singular projective variety defined over k of dimension d. André Weil conjectured in 1949:

- (Rationality) $Z(X,t) = \frac{P(t)}{Q(t)}$ where $P(t), Q(t) \in \mathbb{Q}[t]$.
- (Functional equation) $Z(X, \frac{1}{q^d t}) = \pm q^{d\chi/2} t^{\chi} Z(X,t)$ where $\chi = \Delta \cdot \Delta$ (Euler-Poincaré characteristic).
- (Riemann hypothesis)
$$Z(X,t) = \frac{P_1(t) \cdot P_3(t) \cdot \dots \cdot P_{2d-1}(t)}{P_0(t) \cdot P_2(t) \cdot \dots \cdot P_{2d}(t)}$$
$P_0(t) = 1 - t$, $P_{2d}(t) = 1 - q^d t$, and, for $1 \leqslant r \leqslant 2d-1$:
$$P_r(t) = \prod_{j=1}^{\beta_r} (1 - \alpha_{r,j} t)$$
where $\alpha_{r,j}$ are algebraic integers of absolute value $q^{r/2}$.
- (Betti numbers) Let us call $\beta_r = \deg P_r(t)$ the r^{th} *Betti number*. Then $\chi = \sum_{r=0}^{2d} (-1)^r \beta_r$. Moreover, if Y is a non-singular variety defined over the ring of integers in a number field, then the Betti numbers of the variety X derived by reduction modulo a maximal ideal equals the (usual) Betti numbers of Y as a (complex) manifold for almost all maximal ideals.

1.5. **An example.** Let $X = \mathbb{P}^d_{\overline{k}} = \mathbb{A}^0_{\overline{k}} \coprod \mathbb{A}^1_{\overline{k}} \coprod \mathbb{A}^2_{\overline{k}} \coprod \dots \coprod \mathbb{A}^d_{\overline{k}}$.
$$N_m = 1 + q^m + q^{2m} + \dots + q^{dm}$$
$$\begin{aligned} Z(\mathbb{P}^d_{\overline{k}}, t) &= \exp \sum_{m \geqslant 1} (1 + q^m + q^{2m} + \dots + q^{dm}) \frac{t^m}{m} \\ &= \exp \sum \frac{t^m}{m} \cdot \exp \sum \frac{(qt)^m}{m} \cdot \exp \sum \frac{(q^2 t)^m}{m} \dots \exp \sum \frac{(q^d t)^m}{m} \\ &= \frac{1}{(1-t)(1-qt)(1-q^2t)\dots(1-q^d t)}. \end{aligned}$$
$Z(\mathbb{P}^d_{\overline{k}}, t)$ is rational, and
$$\begin{aligned} Z(\mathbb{P}^d_{\overline{k}}, \frac{1}{q^d t}) &= \frac{1}{(1-\frac{1}{q^d t})(1-\frac{1}{q^{d-1}t})(1-\frac{1}{q^{d-2}t})\dots(1-\frac{1}{t})} \cdot \frac{q^{d(d+1)/2} t^{d+1}}{q^{d(d+1)/2} t^{d+1}} \\ &= (-1)^{d+1} \cdot \frac{q^{d(d+1)/2} t^{d+1}}{(1-q^d t)(1-q^{d-1}t)(1-q^{d-2}t)\dots(1-t)} \\ &= (-1)^{d+1} q^{d\chi/2} t^{\chi} Z(\mathbb{P}^d_{\overline{k}}, t) \end{aligned}$$
so we obtain the functional equation, since $\chi = d+1$. Put $P_r(t) = (1 - q^{r/2} t)$ if $0 \leqslant r \leqslant 2d$ and r is even, and $P_r(t) = 1$ otherwise. Then the Riemann hypothesis is OK.

Finally, for the Betti part; since $\mathbb{P}^d_{\mathbb{C}} = 0\text{-cell} \coprod 2\text{-cell} \coprod 4\text{-cell} \coprod \dots \coprod 2d\text{-cell}$, we get

$$b_r(\mathbb{P}^d_{\mathbb{C}}) = \deg P_r(t) = \beta_r(\mathbb{P}^d_{\overline{k}}) .$$

1.6. **Why "Riemann hypothesis"?** Let X_0 be the scheme over k defined by the same equations as X, then a closed point $x \in X_0$ corresponds to maximal ideal $\mathfrak{m}_x \subseteq A$ where $\operatorname{Spec} A$ is some open sub-set of X_0. By Hilberts Nullstellensatz $k(x) := A/\mathfrak{m}_x$ is a finite field extension k_m of k. I.e. the closed point $x \in \operatorname{Spec} A$ gives a non-unique k-linear ring homomorphism $\varphi : A \to k_m$. If $\sigma \in \operatorname{Gal}(k_m/k)$, then $\sigma\varphi : A \to k_m$ is another k-linear ring homomorphism, and it gives *the same closed point* (same kernel) but *a different* k_m-point. In fact $\operatorname{Gal}(k_m/k)$ is cyclic of order m generated by the Frobenius automorphism $a \mapsto a^q$.

Conclusion: There are m k_m-points in X corresponding to the closed point x in X_0 of degree $m = [k(x) : k]$.

Let $B_r = \#\{x \in X_0 \,|\, x \text{ closed}, \ \deg(x) = r\}$. Since $k_r \subseteq k_m \Leftrightarrow r|m$ we get $N_m = \sum_{r|m} rB_r$.

Definition 2 (by E. Artin for curves over finite fields)**.** If X_0 is a scheme defined over $\mathbb{Z}$ (e.g. over k), let

$$\zeta_{X_0}(s) = \prod_{\substack{x \in X_0 \\ x \text{ closed}}} \frac{1}{1 - \#k(x)^{-s}}$$

which is a holomorphic function for $\Re(s) > \dim X_0$.

$X_0 = \operatorname{Spec} \mathbb{Z}$ gives Riemann's zeta function.

$$\begin{aligned} Z(X,t) &= \exp \sum_{m \geqslant 1} N_m \frac{t^m}{m} \\ &= \exp \sum_{m \geqslant 1} \sum_{r|m} rB_r \frac{t^m}{m} \\ &= \exp \sum_{r,i \geqslant 1} rB_r \frac{t^{ir}}{ir} \\ &= \exp \sum_{r \geqslant 1} B_r \sum_{i \geqslant 1} \frac{t^{ir}}{i} \\ &= \exp \sum_{r \geqslant 1} -B_r \log(1 - t^r) \\ &= \prod_r \frac{1}{(1-t^r)^{B_r}} \qquad \text{(let } t = q^{-s}) \\ &= \prod_r \frac{1}{(1-q^{-rs})^{B_r}} \end{aligned}$$

$$= \prod_{\substack{x \in X_0 \\ x \text{ closed}}} \frac{1}{1 - \#k(x)^{-s}}$$

$$= \zeta_{X_0}(s)$$

By Weil's RH $\zeta_{X_0}(s)$ has its poles on the lines $\Re(s) = 0, 1, 2, \dots, \dim X$ and its zeros on the lines $\Re(s) = 1/2, 3/2, 5/2, \dots, \dim X - 1/2$.

In particular; for *curves* the zeros (a finite number!) are on the line $\Re(s) = 1/2$.

2. Weil's idea

2.1. **The Frobenius.** The $\overline{k}$-linear *Frobenius* endomorphism $F : X \to X$ is locally defined as $X(\overline{k}) \ni a = (a_1, \dots, a_n) \mapsto F(a) = (a_1^q, \dots, a_n^q) \in X(\overline{k})$:

$$f_i(a_1, \dots, a_n) = 0 \Rightarrow f_i(a_1^q, \dots, a_n^q) = f_i(a_1, \dots, a_n)^q = 0$$

since the coefficients of the f_i are contained in k.

Also

$$a \in X(k) \Leftrightarrow F(a) = a$$

since $k^\times$ is a cyclic group of order $q - 1$, and since $\mathrm{Gal}(\overline{k}/k) \cong \hat{\mathbb{Z}}$ is (pro-finitely) generated by the q-Frobenius. Also

$$a \in X(k_m) \Leftrightarrow F^m(a) = a\,.$$

Hence

$$N_m = \#\text{fixed points of } F^m$$

(—and the fixed points are isolated).

Suppose there was a cohomology theory $\mathrm{H}^*(X)$ *with properties similar to those of singular cohomology*; -a graded algebra contravariant in X (with Gysin map, Künneth formula, Poincaré duality...) over a field Λ of charcteristic 0 ($\Lambda = \mathbb{Q}$ would be ideal). Then one can deduce a *Lefschetz fixed-point formula.* One would have

$$N_m = \sum_{i=0}^{2d} (-1)^r \,\mathrm{Tr}(F^m |\, \mathrm{H}^r(X))\,.$$

Put $P_r(t) = \det(1 - Ft |\, \mathrm{H}^r(X)) = \prod_j (1 - \alpha_{r,j} t)$. The $\alpha_{r,j}$ are the *eigenvalues* of $F |\, \mathrm{H}^r(X)$. Then

$$\mathrm{Tr}(F^m |\, \mathrm{H}^r(X)) = \sum_j \alpha_{r,j}^m\,,$$

hence

$$\sum_{m \geqslant 1} \mathrm{Tr}(F^m |\, \mathrm{H}^r(X)) \frac{t^m}{m} = \sum_j \Big(\sum_{m \geqslant 1} \alpha_{r,j}^m \frac{t^m}{m} \Big) = \log \frac{1}{P_r}$$

so

$$\begin{aligned}
Z(X,t) &= \exp \sum_{m \geqslant 1} N_m \frac{t^m}{m} \\
&= \exp \sum_{m \geqslant 1} \Big(\sum_{r=0}^{2d} (-1)^r \operatorname{Tr}(F^m | \operatorname{H}^r(X)) \Big) \frac{t^m}{m} \\
&= \exp(-\log P_0 + \log P_1 - \log P_2 + \cdots - \log P_{2d}) \\
&= \frac{P_1 P_3 \ldots P_{2d-1}}{P_0 P_2 \ldots P_{2d}} \, .
\end{aligned}$$

Since F acts on the coefficients $\operatorname{H}^0(X) \cong \Lambda$ as id, $P_0 = (1-t)$. If F acts on $\operatorname{H}^{2d}(X) \cong \Lambda$ by $\deg F = q^d$, $P_{2d} = (1 - q^d t)$. Moreover; the functional equation should follow from the Poincaré duality.

A diophantine estimate follows from the equation

$$N_m = 1 + \sum_{r=1}^{2d-1} (-1)^r \sum_j \alpha_{r,j}^m + q^{md}$$

with $|\alpha_{r,j}| \leqslant q^{d-1/2}$, in particular q^{md} is the dominant term.

3. The étale "topology"

3.1. **Problems with the Zariski topology.**

- Non-singular varieties correspond locally to regular rings. There are very many regular rings (e.g. Riemann surfaces).
- $\operatorname{H}^*(X_{\mathrm{Zar}}, \mathbb{Z}) = 0$ for $r > 0$.
- $\operatorname{H}^*(X_{\mathrm{Zar}}, \mathcal{F}) = 0$ for $r > \dim X$.
- $\operatorname{H}^*(X_{\mathrm{Zar}}, \mathcal{F})$ are vector spaces over the ground field (so possibly a mod p Lefschetz).
- No inverse mapping theorem.

(1) $$g : Y \to X \text{ with } T_y g : T_y Y \xrightarrow{\cong} T_{g(y)} X$$

is not necessarily a local isomorphism around y.

3.2. **The étale site.**

Definition 3. $g : Y \to X$ is *étale* if for any $x \in X$ there is an open $x \in \operatorname{Spec} A \subseteq X$ and an open $\operatorname{Spec} B \subseteq Y$ mapping to $\operatorname{Spec} A$ such that $B \cong A[x_1, \ldots, x_N]/(f_1, \ldots, f_N)$ with $\det(\partial f_i / \partial x_j)$ invertible in B.

Remark 1. This definition is good for finite type maps of schemes, and then it is equivalent to g being *flat* and *unramified*. If Y and X are non-singular varieties, it is equivalent to (1) for all $y \in Y$.

Étale maps are open. Étale maps are (locally) the algebraic equivalents of finite (unramified) covering spaces.

Example 2. If g is

$$t \mapsto t^n : \mathbb{A}^1_k \longrightarrow \mathbb{A}^1_k \text{ then } \mathrm{d}(t^n) = nt^{n-1}\mathrm{d}t \neq 0 \text{ if } t \neq 0 \text{ and } p \nmid n$$

and so g restricted to the complement of the origin is étale.

Example 3. $\operatorname{Spec} K \to \operatorname{Spec} k$, i.e $k \hookrightarrow K$ an extension of fields, is étale if K is an *unramified* field extension of k. That is; $K \cong k[t]/(f)$ where $f(t)$ has no multiple roots in $\overline{k}$ (always OK in characteristic 0).

Definition 4. The *étale site* $X_{\text{ét}}$ is the category $\text{Ét}/X$ of étale maps $V \to X$ together with all "coverings" $\{\varphi_i : U_i \xrightarrow{\text{ét}} V\}_{i\in I}$ for all V in $\text{Ét}/X$ such that $\bigcup_{i\in I} \varphi_i(U_i) = V$

Remark that a Zariski covering also is an étale covering. The coverings will be our substitute for a traditional topology, where the "intersection" of $U_1 \to V$ and $U_2 \to V$ is given by the fiber product $U_1 \times_V U_2 \to V$.

3.3. **Sheaves for the étale topology.**

Definition 5. An étale sheaf $\mathcal{F}$ of sets (or abelian groups,...) on X is a contravariant functor

$$\mathcal{F} : \text{Ét}/X \longrightarrow \mathsf{Sets}$$

such that

$$\mathcal{F}(V) \longrightarrow \prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \times_V U_j)$$

is exact.

Some examples:

- $\mathcal{O}_{X_{\text{ét}}}(U \to X) = \Gamma(U, \mathcal{O}_U)$ is an étale sheaf (of rings) by descent of étale maps. Similar for coherent sheaves.
- Any X-scheme $Z \to X$ defines an étale sheaf (of sets) $\mathcal{F}_Z = \operatorname{Hom}_X(-, Z)$ again by descent.
- $\mathbb{G}_m(U \to X) = \Gamma(U, \mathcal{O}_U)^\times$ (invertible elements) is a sheaf of abelian groups. If $k = \overline{k}$ and $n \nmid \operatorname{char}(k)$ there is a short exact sequence

$$0 \to \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{t \mapsto t^n} \mathbb{G}_m \to 0$$

  —the *Kummer sequence*, and μ_n is the torsion sheaf of the n^{th} roots of unity. The surjectivity (and exactness) follows more generally if no residue field of X has characteristic divisible by p.
- Constant sheaves. If M is an abelian group, let $M(U \to X) = M^{\pi_0 U}$

3.4. **Cohomology of étale sheaves.** The category of étale sheaves of abelian groups has enough injectives, and the global sections functor $\Gamma(X,-) : \mathsf{Sh}(X_{\text{ét}}) \to \mathsf{Ab}$ is left exact, so we obtain derived functors

$$\mathrm{H}^r(X_{\text{ét}}, \mathcal{F}) = \mathrm{H}^r(\Gamma(X, \mathcal{I}^{\cdot}))$$

where $0 \to \mathcal{F} \to \mathcal{I}^0 \to \mathcal{I}^1 \to \dots$ is an injective resolution of $\mathcal{F}$.

- Some analogs of the Eilenberg-Steenrod axioms hold.
- If $X = \operatorname{Spec} k$ one obtains *Galois cohomology* of fields.
- Still problems, e.g. $\mathrm{H}^1(X_{\text{ét}}, \mathbb{Z}) = 0$. Torsion sheaves give more.

3.5. ***l*-adic cohomology.**

Definition 6. Let $X/\overline{k}$ be a variety, l a prime number, $l \neq p$, set $\mathbb{Z}_l := \varprojlim \mathbb{Z}/l^n\mathbb{Z}$ and let $\mathbb{Q}_l$ be the fraction field. Then

$$\mathrm{H}^r(X, \mathbb{Z}_l) := \varprojlim \mathrm{H}^r(X_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z})$$

and *l-adic cohomology* is

$$\mathrm{H}^r(X) = \mathrm{H}^r(X, \mathbb{Q}_l) := \mathrm{H}^r(X, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \,.$$

We also have cohomology with compact support;

$$\mathrm{H}^r_c(X) = \varprojlim \mathrm{H}^r(X_{\text{ét}}, j_! \mathbb{Z}/l^n\mathbb{Z}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

where $j_!$ is an "extension by zero"-functor and $j : X \hookrightarrow \overline{X}$ is (any) embedding of X in a complete variety $\overline{X}$.

Remark that $\mathrm{H}^r(X_{\text{ét}}, j_! \mathbb{Z}/l^n\mathbb{Z})$ is not a derived functor, but is independent of j (which always exists).

Properties of l-adic cohomology.

- $\mathrm{H}^r(X)$ is a contravariant functor in X of $\mathbb{Q}_l$ vector spaces, which are finite dimensional if X is complete. There is also a continuous action of $\mathrm{Gal}(\overline{k}/k)$ on $\mathrm{H}^r(X)$.

$$\mathrm{H}^r(X) \neq 0 \Longrightarrow 0 \leqslant r \leqslant 2d$$

and

$$X \text{ affine and } \mathrm{H}^r(X) \neq 0 \Longrightarrow 0 \leqslant r \leqslant d$$

- There is a cup product $\mathrm{H}^r(X) \times \mathrm{H}^s(X) \xrightarrow{\cup} \mathrm{H}^{r+s}(X)$ which makes $\mathrm{H}^*(X)$ a graded commutative $\mathbb{Q}_l$-algebra. One has a *Künneth formula* $\mathrm{H}^*(X) \otimes_{\mathbb{Q}_l} \mathrm{H}^*(Y) \xrightarrow{\simeq} \mathrm{H}^*(X \times Y)$.
- If X and Z are non-singular varieties, $Z \subseteq X$ of codimension c, then there is a *Gysin isomorphism*

$$\mathrm{H}^{r-2c}(Z, \mathbb{Q}_l(-c)) \xrightarrow{\simeq} \mathrm{H}^r_Z(X) \quad \text{(support in } Z\text{)}.$$

The twist is comming into the limiting process by tensorisation with the free rank 1 $\mathbb{Z}/l^n\mathbb{Z}$-module $\mathrm{Hom}_{\mathbb{Z}/l^n\mathbb{Z}}(\mu_{l^n}^{\otimes c}, \mathbb{Z}/l^n\mathbb{Z})$, one has $\mathbb{Q}_l(\pm c) \cong \mathbb{Q}_l$

non-canonically. Replacing $\mathrm{H}^r_Z(X)$ in the long-exact sequence of the pair $(X, X\backslash Z)$ with $\mathrm{H}^{r-2c}(Z, \mathbb{Q}(-c))$ gives $(U = X\backslash Z)$

$$\mathrm{H}^r(X) \xrightarrow{\simeq} \mathrm{H}^r(U)\,, \quad 0 \leqslant r < 2c-1$$

and a long-exact *Gysin sequence*

$$0 \to \mathrm{H}^{2c-1}(X) \to \mathrm{H}^{2c-1}(U) \to \dots$$
$$\dots \to \mathrm{H}^{r-2c}(Z, \mathbb{Q}(-c)) \to \mathrm{H}^r(X) \to \mathrm{H}^r(U) \to \dots$$

• Assume X is non-singular. The r^{th} *Chow group* $\mathrm{CH}^r(X)$ is the free abelian group generated by codimension r sub-varieties of X modulo rational equivalence. Let $Z_1 \sim Z_2$ if there is a codimension r sub-variety $W \subseteq X \times \mathbb{P}^1_{\bar{k}}$ such that the induced map $W \to \mathbb{P}^1_{\bar{k}}$ is dominant with Z_i as fibers (counted with multiplicity) over closed points in $\mathbb{P}^1_{\bar{k}}$. Rational equivalence is generated by $\sim$. There is an intersection product $\mathrm{CH}^r(X) \times \mathrm{CH}^s(X) \to \mathrm{CH}^{r+s}(X)$ making $\mathrm{CH}^*(X)$ a commutative and graded ring. There is a *cycle map* from the Chow ring

$$\mathrm{cl}_X : \mathrm{CH}^*(X) \to \oplus\, \mathrm{H}^{2r}(X, \mathbb{Q}_l(r))$$

which is a homomorphism of graded rings. If Z is a non-singular sub-variety of X, then $\mathrm{cl}_X(Z)$ is the image of 1 under the Gysin map

$$\mathbb{Q}_l = \mathrm{H}^0(Z) \xrightarrow{\simeq} \mathrm{H}^{2c}_Z(X, \mathbb{Q}_l(c)) \to \mathrm{H}^{2c}(X, \mathbb{Q}_l(c))\,.$$

E.g. we have

$$\mathrm{CH}^1(X) = \mathrm{Pic}\, X = \mathrm{H}^1(X_{\text{ét}}, \mathbb{G}_m)\,,$$

the connecting map

$$\mathrm{H}^1(X_{\text{ét}}, \mathbb{G}_m) \xrightarrow{\partial} \mathrm{H}^2(X_{\text{ét}}, \mathbb{Q}_l(1))$$

arising from the Kummer sequences gives

$$\mathrm{cl}_X : \mathrm{CH}^1(X) \longrightarrow \mathrm{H}^2(X_{\text{ét}}, \mathbb{Q}_l(1))\,.$$

• If $Z = P$ a point, the canonical isomorphism

$$\eta(X) : \mathrm{H}^{2d}_c(X, \mathbb{Q}_l(d)) \xrightarrow{\simeq} \mathbb{Q}_l\,.$$

is defined by $\mathrm{cl}_X(P) \mapsto 1$. There are canonical perfect pairings (*Poincaré duality*)

$$\mathrm{H}^r_c(X, \mathbb{Q}_l) \times \mathrm{H}^{2d-r}(X, \mathbb{Q}_l(d)) \longrightarrow \mathrm{H}^{2d}_c(X, \mathbb{Q}_l(d)) \xrightarrow{\eta(X)} \mathbb{Q}_l$$

We get defined a *push forward for proper maps* via the Poincaré duality.

• A *Lefschetz fixed-point formula* now follows: Assume $\varphi : X \to X$ is an endomorphism of a complete non-singular variety $X/\bar{k}$. Then

$$\Gamma_\varphi \cdot \Delta = \sum_{r=0}^{2d} (-1)^r \,\mathrm{Tr}(\varphi |\, \mathrm{H}^r(X, \mathbb{Q}_l))$$

where Γ_φ is the graph of φ and Δ is the graph of id_X. E.g. $\Delta \cdot \Delta = \chi_l$.

• These results are based on (hard) *base change theorems* (proper, smooth and proper-smooth).

4. What is obtained so far?

For a complete, non-singular variety $X/\overline{k}$ we have

4.1. **Rationality.**

$$Z(X,t) = \frac{P_{1,l}(t)\cdot P_{3,l}(t)\cdot\dots\cdot P_{2d-1,l}(t)}{P_{0,l}(t)\cdot P_{2,l}(t)\cdot\dots\cdot P_{2d,l}(t)}$$

with $P_{r,l}(t) = \det(1-Ft|\,\mathrm{H}^r(X,\mathbb{Q}_l)) \in \mathbb{Q}_l[t]\cap\mathbb{Q}[[t]] = \mathbb{Q}(t)$. Remember (regarding X_0/k)

$$Z(X,t) = \prod_{\substack{x\in X_0\\ x\text{ closed}}} \frac{1}{1-t^{\deg(x)}} \in \mathbb{Z}[[t]]\,,$$

so if $Z(X,t)=P(t)/Q(t)$, $P = 1+t\cdot\dots$ and $Q = 1+t\cdot\dots$ are prime, then $P,Q\in\mathbb{Z}[t]$.

Moreover; F^* acts as identity on H^0 and as q^d on H^{2d}. We obtain

$$P_0(t) = 1-t \qquad P_{2d}(t) = 1-q^dt\,.$$

4.2. **Functional equation.** If, by Poincaré duality, $\eta_X(y\cup x)=1$, by definition $\eta_X(y\cup F^*(x)) = \eta_X(F_*(y)\cup x)$, so F_* has the same eigenvalues as F^*. If the eigenvalues of F^* acting on $\mathrm{H}^r(X)$ is $\alpha_1,\dots,\alpha_s$, then the eigenvalues of F^* acting on $\mathrm{H}^{2d-r}(X)$ is $q^d/\alpha_1,\dots,q^d/\alpha_s$ since $\eta_X(F_*F^*(y)\cup x) = \eta_X(F^*(y)\cup F^*(x)) = \eta_X(F^*(y\cup x)) = q^d$.

So, if $P_r(t) = \prod(1-\alpha_{r,j}t)$, then $P_{2d-r}(t) = \prod(1-\frac{q^d}{\alpha_{r,j}}t)$ and we obtain

$$P_{2d-r}(1/q^dt) = \prod(1-\frac{q^d}{\alpha_{r,j}}\frac{1}{q^dt}) = (-1)^{\beta_r}\cdot(\prod\alpha_{r,j})^{-1}t^{-\beta_r}P_r(t)$$

and

$$P_r(1/q^dt) = (-1)^{\beta_r}\cdot(\prod\alpha_{r,j})q^{-d\beta_r}t^{-\beta_r}P_{2d-r}(t)\,.$$

The $\prod\alpha_{r,j}$-terms cancel in $Z(X,t)$ if $r\neq d$. If $r=d$ then $(\prod\alpha_{r,j})(\prod d^q/\alpha_{r,j}) = q^{d\beta_d}$, so $\prod\alpha_{r,j} = \pm q^{d\beta_d/2}$. We get

$$\begin{aligned} Z(X,1/q^dt) &= \pm\prod_{r=0}^{2d}(P_{2d-r}(1/q^dt)P_r(1/q^dt))^{(-1)^r/2} \\ &= \pm q^{d\chi/2}t^{\chi}Z(X,t)\,. \end{aligned}$$

For the sign; it is only the middle cohomology which contributes since $\beta_r+\beta_{2d-r}$ is even. For the middle cohomology the eigenvalues come in complex conjungate pairs or as $\pm q^{d/2}$. For d odd the perfect pairing is skew symmetric, so *all* eigenvalues come in pairs and β_d is even, so the sign is $+1$. For d even the overall sign is $(-1)^{\xi+\beta_d}$ if the number of eigenvalues $-q^{d/2}$ is ξ.

4.3. **Riemann hypothesis implies $P_{r,l}(t)$ independent of l.** Since $\prod_{r \text{ odd(even)}} P_{r,l}(t) \in 1 + t \cdot \mathbb{Z}[t]$, the inverse roots of $P_{r,l}(t)$ are algebraic integers, so $P_{r,l}(t) \in 1 + t \cdot \mathbb{Z}[t]$ and is characterised independently of l as the numerator or denominator of $Z(X, t)$ whose inverse roots have absolute value $q^{r/2}$.

4.4. **Betti numbers.** The Lefschetz fixed-point formula gives

$$\chi = \sum_{r=0}^{2d} (-1)^r \dim \mathrm{H}^r(X, \mathbb{Q}_l)\,.$$

Theorem 1. *If a variety $X/\overline{k}$ can be lifted to characteristic 0; i.e. there exists a characteristic 0 DVR R, $K = K(R)$, with $R/\mathfrak{m}_R = \overline{k}$ and $\mathcal{X} \to \operatorname{Spec} R$ proper and smooth with closed fiber $X \to \operatorname{Spec} \overline{k}$, then*

$$\mathrm{H}^r(X_{\acute{e}t}, \mathbb{Q}_l) \cong \mathrm{H}^r(\mathcal{X}_{\overline{K}\,\acute{e}t}, \mathbb{Q}_l)$$

Remark that there in general are obstructions for lifting a variety to characteristic 0.

Theorem 2. *Let $X/\mathbb{C}$ be a (non-singular) variety and X^{an} the corresponding complex analytic space, then*

$$\mathrm{H}^r(X_{\acute{e}t}, \mathbb{Q}_l) \cong \mathrm{H}^r_{sing}(X^{an}, \mathbb{Q}_l)$$

Corollary 1. *If Y is a smooth complete variety defined by equations with coefficients in a ring of integers $\mathcal{O}$ of a number field and reduction modulo $\mathfrak{m} \subseteq \mathcal{O}$ gives a non-singular variety X (defined over the finite field $\mathcal{O}/\mathfrak{m}$) then*

$$\dim \mathrm{H}^r(Y^{an}, \mathbb{Q}) = \deg P_{r,l}(X, t)\,.$$

Remark that for $r = 1$ Theorem 2 is the Riemann Existence Theorem.

5. A reduction of the Riemann hypothesis

Proposition 1. *The Riemann hypothesis holds for all non-singular projective varieties, if, for any non-singular projective variety X of even dimension d, every eigenvalue α of F acting on $\mathrm{H}^d(X, \mathbb{Q}_l)$ (the middle cohomology) is an algebraic number with*

$$q^{d/2-1/2} \leqslant |\alpha'| \leqslant q^{d/2+1/2}$$

for all the conjungates α' of α.

Proof. Assume Y is non-singular, projective, $\dim Y = d$ (not necessarily even), α an eigenvalue of $F|\,\mathrm{H}^d(Y)$. Then

$$\mathrm{H}^{dm}(Y^m) \cong \mathrm{H}^d(Y) \otimes \mathrm{H}^d(Y) \otimes \ldots \otimes \mathrm{H}^d(Y) \oplus \ldots \quad \text{(Künneth formula)}$$

so that α^m is an eigenvalue of $F|\,\mathrm{H}^{dm}(Y^m)$. By assumption (m even)

$$q^{md/2-1/2} \leqslant |\alpha'|^m \leqslant q^{md/2+1/2}$$

hence $|\alpha'| = q^{d/2}$.

If α is an eigenvalue of $F|\,\mathrm{H}^r(X)$ then q^d/α is an eigenvalue of $F|\,\mathrm{H}^{2d-r}(X)$, hence we may assume $r > d$. By Bertini there is a hyperplane $H \subseteq \mathbb{P}^n_k$ such that $Z := H \bigcap X$ is non-singular. Replacing k by a finite extension k_m and F by F^m changes the eigenvalues $\alpha \mapsto \alpha^m$, however

$$|\alpha^m| = (q^m)^{r/2} \Leftrightarrow |\alpha| = q^{r/2}\,.$$

Hence we may assume H (and so Z) is defined over k. The Gysin sequence gives

$$\ldots \to \mathrm{H}^{r-2}(Z, \mathbb{Q}_l(-1)) \xrightarrow{i_*} \mathrm{H}^r(X, \mathbb{Q}_l) \to \mathrm{H}^r(X\backslash Z, \mathbb{Q}_l) \to \ldots\,,$$

but $X \setminus Z$ is affine and $r > \dim X$ so $\mathrm{H}^r(X \setminus Z, \mathbb{Q}_l) = 0$. By induction on d the eigenvalues of $F|\,\mathrm{H}^{r-2}(Z)$ are algebraic integers of absolute value $q^{r/2-1}$. Now

$$F_X^* \circ i_* = q \cdot i_* \circ F_Z^*$$

and i_* is surjective so $F|\,\mathrm{H}^r(X)$ has algebraic integers as eigenvalues with absolute value $q{\cdot}q^{r/2-1} = q^{r/2}$. The start of the induction is trivial for $d = 0$, and $d = 1$ is odd! □

6. History and references

André Weil stated his conjectures in 1949 [19]. He had already in 1940-41 sketched two proofs for curves, [15, 16], the first completed and generalised to abelian varieties in [18], the second completed in [17]. H. Hasse had given two proofs for elliptic curves in the 1930s. It was E. Artin who introduced the zeta function in 1924 for function fields of curves over finite fields (only for hyperelliptic curves according to S. Kleiman [9]) and conjectured its zeros to lie on the circle $|t| = q^{1/2}$. F. K. Schmidt established the rationality and the functional equation for curves in 1931.

In 1960 B. Dwork proved that the zeta function of a (not necessarily complete) variety was rational by p-adic analysis [5]. By 1963 M. Artin and A. Grothendieck had developed enough of the étale cohomology to give the Lefschetz interpretation of the P_r and thus obtain the results refered in Section 4, see [10, 11, 12]. Some special cases of the Weil conjectures where obtained; cubic threefolds by E. Bombieri and H. P. F. Swinnerton-Dyer in 1967 [1], unirational projective threefolds by Ju. I. Manin in 1968 [13], $K3$-surfaces and complete intersections by P. Deligne in 1972, [2, 3]. The proof of the Riemann hypothesis, which completed the proof of the Weil conjectures, was published by Deligne in 1974 [4].

An overview of Deligne's proof together with historical remarks (including the missing references above) is given by N. Katz in [8], historical remarks are also found in the forword by J. A. Dieudonné in [6].

My main source for this résymé is the lecture notes of J. S. Milne which are available at his private web page [14], together with Appendix C in R. Hartshorne's book [7].

References

[1] E. Bombieri and H. P. F. Swinnerton-Dyer, *On the local zeta function of a cubic threefold*, Ann. Scuola Norm. Sup. Pisa (3) **21** (1967), 1–29. MR 35 #2894

[2] Pierre Deligne, *La conjecture de Weil pour les surfaces $K3$*, Invent. Math. **15** (1972), 206–226. MR 45 #5137

[3] ———, *Les intersections complètes de niveau de Hodge un*, Invent. Math. **15** (1972), 237–250. MR 46 #189

[4] ———, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. MR 49 #5013

[5] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR 25 #3914

[6] Eberhard Freitag and Reinhardt Kiehl, *Étale cohomology and the Weil conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 13, Springer-Verlag, Berlin, 1988, Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné. MR **89f:**14017

[7] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, no. 52, Springer-Verlag, 1977.

[8] Nicholas M. Katz, *An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, R.I., 1976, pp. 275–305. MR 54 #12780

[9] Steven L. Kleiman, *The standard conjectures*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 3–20. MR **95k:**14010

[10] J. L. Verdier M. Artin, A. Grothendieck, *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat, Lecture Notes in Mathematics, Vol. 269. MR 50 #7130

[11] ———, *Théorie des topos et cohomologie étale des schémas. Tome 2*, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat, Lecture Notes in Mathematics, Vol. 270. MR 50 #7131

[12] ———, *Théorie des topos et cohomologie étale des schémas. Tome 3*, Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat, Lecture Notes in Mathematics, Vol. 305. MR 50 #7132

[13] Ju. I. Manin, *Correspondences, motifs and monoidal transformations*, Mat. Sb. (N.S.) **77 (119)** (1968), 475–507. MR 41 #3482

[14] James S. Milne, *Lectures on etale cohomology*, www.jmilne.org, August 1998.

[15] André Weil, *Sur les fonctions algébriques à corps de constantes fini*, C. R. Acad. Sci. Paris **210** (1940), 592–594. MR 2,123d

[16] ______, *On the Riemann hypothesis in functionfields*, Proc. Nat. Acad. Sci. U. S. A. **27** (1941), 345–347. MR 2,345b

[17] ______, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948. MR 10,262c

[18] ______, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946), Hermann & Cie., Paris, 1948. MR 10,621d

[19] ______, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. MR 10,592e

Dept. of Mathematics, University of Oslo, PO Box 1053 Blindern, NO-0316 Oslo, NORWAY

E-mail address: `ile@math.uio.no`